Claims

What is claimed is:

1. A method of implementing a cryptographic protocol between multiple parties including at least a prover and a verifier, the method comprising the steps of:

generating at least one signal corresponding to information representative of first and second proofs based on an operation associated with the cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed; and

transmitting the proof information signal from the prover to the verifier, such that the verifier can determine if the operation associated with the cryptographic protocol is valid based at least in part on the proof information signal.

2. The method of claim 1 wherein the operation associated with the cryptographic protocol is an exponentiation operation, and the proof information signal is based on a randomized instance of the exponentiation operation.

3. The method of claim 1 wherein the first proof is a blinded proof configured so as to prevent leaks of information relating to the cryptographic protocol.

4. The method of claim 1 further including the step of generating an indication that the operation was correctly performed if the first and second proofs are acceptable to the verifier.

5. The method of claim 1 further including the step of generating an indication that the operation was not correctly performed if the first proof is not acceptable to the verifier but the second proof is acceptable to the verifier.

6. The method of claim 1 wherein further including the step of generating an indication that the prover is cheating if the second proof is not acceptable to the verifier.

7. The method of claim 1 wherein the prover is given a quadruple (g, y, m, s), and needs to prove to the verifier that $\log_g y = \log_m s$, the prover knows x, the discrete logarithm of y with respect to g, and the method further includes the steps of:

the prover randomly selecting a number a;

the prover generating a first signal corresponding to information representative of the first proof as a triple $(\bar{s}, \bar{\sigma}, \bar{m}) = (s^a, m^{ax}, m^a)$;

the verifier accepting the first proof if and only if $\bar{s} = \bar{\sigma}$;

the prover generating a second signal corresponding to information representative of the second proof as an indication that $\log_{\bar{m}} m = \log_{\bar{s}} s$ and that $\log_g y = \log_{\bar{m}} \bar{\sigma}$;

the verifier accepting the second proof if and only if both equations are valid; and

the verifier outputting at least one of: (i) an indication of valid exponentiation if both the first and second proofs are accepted; (ii) an indication that the exponentiation is invalid if the first proof is rejected and the second proof is accepted; and (iii) an indication that the prover is cheating if the second proof is rejected.

8. The method of claim 1 further including the steps of:

applying a key transformation protocol which takes an input of the form (g, y, m, s), for which $\log_g y = \log_m s$, and produces a pair (G, Y) wherein G is a generator and Y is a public key, such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$;

generating a signal corresponding to information representative of the second proof as a digital signature generated using the pair (G, Y) ; and

accepting the second proof if and only if the corresponding digital signature is valid.

9. The method of claim 8 wherein the key transformation protocol takes an input of the form (g, y, m, s, x) for which $\log_g y = \log_m s = x$ and generates the triple (G, Y, X) wherein X is a secret key, such that $Y = G^X$, and the digital signature is generated using the triple (G, Y, X).

10. The method of claim 1 wherein the prover is a distributed prover distributed over multiple machines.

11. An apparatus for implementing a cryptographic protocol between multiple parties including at least a prover and a verifier, the apparatus comprising:

a processor associated with the prover and operative to generate at least one signal corresponding to information representative of first and second proofs based on an operation associated with the cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed, wherein the proof information signal is transmitted from the prover to the verifier and used to determine if the operation associated with the cryptographic protocol is valid; and

a memory coupled to the processor for at least temporarily storing at least a portion of the proof information signal.

12. The apparatus of claim 11 wherein the operation associated with the cryptographic protocol is an exponentiation operation, and the proof information signal is based on a randomized instance of the exponentiation operation.

13. The apparatus of claim 11 wherein the first proof is a blinded proof configured so as to prevent leaks of information relating to the cryptographic protocol.

14. The apparatus of claim 11 wherein the verifier is operative to generate an indication that the operation was correctly performed if the first and second proofs are acceptable to the verifier.

15. The apparatus of claim 11 wherein the verifier is operative to generate an indication that the operation was not correctly performed if the first proof is not acceptable to the verifier but the second proof is acceptable to the verifier.

16. The apparatus of claim 11 wherein the verifier is operative to generate an indication that the prover is cheating if the second proof is not acceptable to the verifier.

17. The apparatus of claim 11 wherein the prover is given a quadruple (g, y, m, s), and needs to prove to the verifier that $\log_g y = \log_m s$, the prover knows x, the discrete logarithm of y with respect to g, and the method further includes the steps of:

the prover randomly selecting a number a;

the prover generating a first signal corresponding to information representative of the first proof as a triple $(\bar{s}, \bar{\sigma}, \bar{m}) = (s^a, m^{ax}, m^a)$;

the verifier accepting the first proof if and only if $\bar{s} = \bar{\sigma}$;

the prover generating a second signal corresponding to information representative of the second proof as an indication that $\log_{\bar{m}} m = \log_{\bar{s}} s$ and that $\log_g y = \log_{\bar{m}} \bar{\sigma}$;

the verifier accepting the second proof if and only if both equations are valid; and

the verifier outputting at least one of: (i) an indication of valid exponentiation if both the first and second proofs are accepted; (ii) an indication that the exponentiation is invalid if the first proof is rejected and the second proof is accepted; and (iii) an indication that the prover is cheating if the first proof is accepted and the second proof is rejected.

18. The apparatus of claim 11 wherein the processor is further operative:

to apply a key transformation protocol which takes an input of the form (g, y, m, s), for which $\log_g y = \log_m s$, and produces a pair (G, Y) wherein G is a generator and Y is a public key, such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$; and

to generate a signal corresponding to information representative of the second proof as a digital signature generated using the pair (G, Y); such that the verifier accepts the second proof if and only if the corresponding digital signature is valid.

19. The apparatus of claim 18 wherein the key transformation protocol takes an input of the form (g, y, m, s, x) for which $\log_g y = \log_m s = x$ and generates the triple (G, Y, X) wherein X is a secret key, such that $Y = G^X$, and the digital signature is generated using the triple (G, Y, X).

20. The apparatus of claim 11 wherein the prover is a distributed prover distributed over multiple machines, and wherein one of the machines includes the processor.

21. The apparatus of claim 11 wherein the prover is a distributed prover distributed over multiple machines, and wherein the processor comprises a distributed processor including at least a portion of a processor associated with each of at least a subset of the multiple machines.

22. A computer-readable medium containing one or more programs, wherein the one or more programs when executed in a computer provide the steps of:

generating at least one signal corresponding to information representative of first and second proofs based on an operation associated with the cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed; and

transmitting the proof information signal from the prover to the verifier, such that the verifier can determine if the operation associated with the cryptographic protocol is valid based at least in part on the proof information signal.

23. A method for implementing a cryptographic protocol between multiple parties including at least a prover and a verifier, the method comprising the steps of:

applying a key transformation protocol which takes an input of the form (g, y, m, s), for which $\log_g y = \log_m s$, and produces a pair (G, Y) wherein G is a generator and Y is a public key, such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$; and

generating a digital signature using the pair (G, Y).

24. An apparatus for implementing a cryptographic protocol between multiple parties including at least a prover and a verifier, the apparatus comprising:

a processor associated with the prover and operative: (i) to apply a key transformation protocol which takes an input of the form (g, y, m, s), for which $\log_g y = \log_m s$, so as to produce a pair (G, Y) wherein G is a generator and Y is a public key, such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$; and (ii) to generate a digital signature using the pair (G, Y).

25. A method of implementing a cryptographic protocol between multiple parties including at least a prover and a verifier, the method comprising the steps of:

receiving at least one signal corresponding to information representative of first and second proofs based on an operation associated with the cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed; and

determining if the operation associated with the cryptographic protocol is valid based at least in part on the proof information signal.

26. An apparatus for implementing a cryptographic protocol between multiple parties including at least a prover and a verifier, the apparatus comprising:

a processor associated with the verifier and operative: (i) to receive at least one signal corresponding to information from the prover representative of first and second proofs based on an operation associated with the cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed, and (ii) to determine if the operation associated with the cryptographic protocol is valid based at least in part on the proof information signal; and

a memory coupled to the processor for at least temporarily storing at least a portion of the proof information signal.

27. A computer-readable medium containing one or more programs, wherein the one or more programs when executed in a computer provide the steps of:

receiving at least one signal corresponding to information representative of first and second proofs based on an operation associated with the cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed; and

determining if the operation associated with the cryptographic protocol is valid based at least in part on the proof information signal.